EUROPEAN
COMMISSION

Brussels, XXX
[…](2025) XXX draft

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of the plan for peer review

This draft has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the establishment of the plan for peer review

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[1], and in particular Article 59(5) thereof,

Whereas:

(1) Pursuant to Article 59(4) of Regulation (EU) 2019/881, peer reviews of national cybersecurity certification authorities (NCCAs) are to be carried out by two NCCAs from other Member States and the Commission. With a view to achieving equivalent standards in respect of European cybersecurity certificates and EU statements of conformity, the Commission should monitor aspects related to compliance with this Regulation and ensure that peer reviews are carried out in a consistent manner throughout the Union. In order to help identify good practices, challenges and lessons learned from the implementation of European cybersecurity certification schemes, the European Union Agency for Cybersecurity (ENISA) should have the opportunity to participate in the peer reviews as an observer. To support the harmonised implementation of the provisions of this Regulation, ENISA, in cooperation with the Commission and the European Cybersecurity Certification Group (ECCG), should also be allowed to develop templates.

(2) In order to ensure predictable planning and the efficient allocation of resources, the peer reviews of each NCCA should be carried out in accordance with an established schedule. It should be possible for an NCCA to request to delay its peer review in exceptional circumstances, such as unexpected staff shortages or instances of *force majeure*. To that effect, it is necessary to set out the arrangements for assessing that request, ensuring that the overarching schedule is maintained, and the objectives of the peer review mechanism are not compromised.

(3) In order to ensure that all Member States contribute to the implementation of the peer-review mechanism, as well as to enable them to benefit from peer-learning, the NCCAs of each Member State should carry out two peer reviews over a five-year period. A rotation system to enable the NCCAs of all Member States to organise their participation should therefore be set up. It is also necessary to set out criteria that NCCAs should take into account when selecting representatives to perform peer reviews, with the objective of ensuring adequate expertise and competence. NCCAs should also be allowed to participate in peer reviews as observers, for the purposes of

[1] OJ L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

monitoring and learning from the process. In such cases, it should not be required for their representative to have the same expertise and competence that is expected of representatives of NCCAs performing the peer reviews.

(4) In order to ensure that an NCCA is peer-reviewed by at least one NCCA employing the same approach on the issuance of certificates at level 'high', ENISA should indicate, when inviting NCCAs to express their interest in being peer-reviewers, whether the peer-reviewed NCCA directly issues certificates at level 'high', makes use of the prior approval model referred to in Article 56(6), point (a), of Regulation (EU) 2019/881, grants a general delegation in accordance with point (b) of that paragraph, or has a combination of these characteristics.

(5) In order to ensure common evaluation criteria and procedures for the operation of peer reviews across the Union, each peer review should always include a self-assessment questionnaire, a documentation review and an on-site visit, accompanied by interviews. After the on-site visit, the peer-review team should discuss the findings with the peer-reviewed NCCA, prepare a draft report and submit it to the peer-reviewed NCCA for comments, with a view to ensuring consensus, where possible. The peer-review team should submit the final report to the ECCG, which should draw up a summary report to be made publicly available.

(6) In order to ensure that the information obtained through the peer-review process is handled in a secure manner, the peer-review team should ensure the use of secure channels of communication such as a secure platform for document storage and sharing, and the use of the appropriate safeguards for confidential data shared between members of the peer-review team. ENISA, taking into account the existing best practices of the NCCAs, should also be able to develop guidelines on how to ensure secure communication, in particular with a view to ensuring that the level of security applied by the peer-review team when collecting, sharing and processing information is aligned with the security needs of the peer-reviewed NCCA.

(7) In order to facilitate cooperation and effective exchange of information between NCCAs, the ECCG, in particular its subgroup on peer review, should contribute to the development of templates as well as assist the Commission with the implementation of this Regulation.

(8) The peer review mechanism constitutes a trans-European digital public service in the meaning of Regulation (EU) 2024/903 of the European Parliament and of the Council[2]. This Regulation introduces new binding requirements affecting that service, and, as such, is subject to the interoperability assessment obligation under Article 3 of Regulation (EU) 2024/903. Accordingly, an interoperability assessment has been carried out, and the resulting report is to be published on the Interoperable Europe Portal.

(9) In the development of this Regulation, the Commission has taken into account the views of the ECCG, including its subgroup on peer review.

(10) The measures provided for in this Regulation are in accordance with the opinion of the Committee established by Article 66 of Regulation (EU) 2019/881,

[2] Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

HAS ADOPTED THIS REGULATION:

Article 1

Schedule, frequency and cost of the peer reviews

1. The peer reviews of the national cybersecurity certification authorities (NCCAs) shall be carried out in accordance with the schedule set out in Annex I. Each peer review shall be completed by the date indicated in that schedule and it shall thereafter be carried out once every five years.

2. In exceptional circumstances, a peer-reviewed NCCA may submit a duly justified request to the Commission to postpone its peer review beyond the date indicated in the schedule set out in Annex I. The Commission shall, in cooperation with the European Cybersecurity Certification Group (ECCG) established by Article 62 of Regulation (EU) 2019/881, assess the request and inform all relevant parties of the outcome in a timely manner.

3. Where a Member State, in accordance with Article 58(1) of Regulation (EU) 2019/881, has designated:

   (a) more than one NCCA in its territory, all the NCCAs of that Member State shall be peer reviewed in parallel;

   (b) the NCCA or NCCAs of another Member State, that NCCA or those NCCAs may be peer reviewed in accordance with the schedule laid down either for the designating Member State or for the Member State of the designated NCCA or NCCAs, with regard to the supervisory tasks carried out in the designating Member State.

4. The European Union Agency for Cybersecurity (ENISA) shall make the following information publicly available on the website on European cybersecurity certification schemes created pursuant to Article 50 of Regulation (EU) 2019/881:

   (a) the information on the schedule set out in Annex I;

   (b) the list of peer-reviewer NCCAs maintained pursuant to Article 2(5).

5. Each NCCA involved in the peer-review process shall bear its own participation costs.

Article 2

Rotation system for peer-reviewer NCCAs

1. In accordance with Article 59(4) of Regulation (EU) 2019/881, each peer review shall be carried out by two peer-reviewer NCCAs of other Member States and the Commission. The NCCAs of each Member State shall participate in the peer review of at least two NCCAs during the each period set out in Annex I.

2. The NCCAs of other Member States may participate in the peer review as observers with one or more representatives, with the agreement of the peer-reviewed NCCA, the peer-reviewer NCCAs and the Commission.

3. One representative from ENISA may participate in the peer review as an observer. Additional representatives may also participate, with the agreement of the peer-reviewed NCCA, the peer-reviewer NCCAs and the Commission.

4. Observers shall have access to the same information as the other members of the peer-review team, but shall not carry out tasks related to the execution of the peer review.

5. ENISA, in cooperation with the Commission and the ECCG, shall propose and maintain the list of peer-reviewer NCCAs that are to carry out the schedule set out in Annex I. During a given year, ENISA, in cooperation with the Commission, shall ask NCCAs to express their interest in carrying out or participating as observers to the peer reviews of the NCCAs scheduled in Annex I for the following year.

6. Where more than two NCCAs express their interest in carrying out the peer review of the same NCCA, the Commission and ENISA shall consult the interested NCCAs and decide on the peer-review participants.

7. Where, in a given year, there are not enough peer-reviewer NCCAs expressing their interest in carrying out the peer reviews, the Commission shall, after consulting the ECCG, select NCCAs to carry out the peer reviews. In its selection, the Commission shall take into account the obligation of the NCCAs of each Member State to participate in the peer review of at least two NCCAs, referred to in paragraph 1.

Article 3

Criteria on the composition of the peer review team

1. In due time before the start of the peer review, each peer-reviewer NCCA shall designate one representative to carry out the peer review. Peer-reviewer NCCAs may designate more than one representative where that is required to ensure that the peer-review team has the necessary competences to carry out the peer review.

2. The representative of peer-reviewer NCCAs, with the exception of representatives of NCCAs participating as observers, shall satisfy the following criteria:

   (a) have at least two years of experience working for the peer-reviewer NCCA or have participated in at least two peer reviews as observers;

   (b) possess sufficient knowledge of the cybersecurity certification framework set out by Regulation (EU) 2019/881;

   (c) have a good working knowledge of English and, where possible, of one or more of the languages spoken in the Member State of the peer-reviewed NCCAs;

   (d) operate independently from the peer-reviewed NCCA.

3. Peer-reviewer NCCAs shall ensure that any risk of conflict of interest concerning the designated representatives is disclosed to the other NCCAs, the Commission and ENISA, before the start of the peer-review process. The peer-reviewed NCCA may object to the designation of particular representatives in accordance with paragraph 5.

4. The peer-reviewer NCCAs shall choose one representative ('the team leader') from among themselves to coordinate the peer review.

5. The Commission shall provide the peer-reviewed NCCA with the names and contact details of the representatives of the peer-reviewer NCCAs before the start of the peer review process. Where the peer-reviewed NCCA wishes to object to the nomination of one or more representatives, it shall, within two weeks, provide a clear justification to the Commission, inform ENISA and the ECCG, and request that the peer-reviewer NCCA nominate a different representative.

6. Where the procedure set out in paragraph 5 causes undue delays in launching the peer review due to exceptional circumstances, the Commission, in consultation with ENISA and the ECCG, shall decide on the composition of the peer-review team.

Article 4

Methodology for the peer review

1. The peer review shall assess the aspects listed in Annex II, in accordance with Article 59(3) of Regulation (EU) 2019/881.

2. ENISA, in cooperation with the ECCG and the Commission, may develop templates for the assessment of the processes established by the peer-reviewed NCCA.

3. The peer review shall include the following:

   (a) a self-assessment questionnaire;

   (b) an assessment of relevant documentation;

   (c) online or physical interviews, or both;

   (d) an on-site visit.

4. The length of the peer review may be agreed beforehand between the peer-review team and the peer-reviewed NCCA, depending on the size and complexity of the activities of the peer-reviewed NCCA. The on-site visit shall not last longer than three working days.

5. Unless otherwise agreed by the peer-review team, the peer-reviewed NCCA and the Commission, the language of cooperation shall be English. The peer-review report referred to in Article 5 shall be drawn up at least in English.

6. The peer-reviewed NCCA shall cooperate and provide the peer-review team with access to the information and documents that are necessary to carry out the peer review. The peer-reviewed NCCA shall submit the self-assessment questionnaire and the latest annual summary report adopted in accordance with Article 58(7), point (g), of Regulation (EU) 2019/881 at least 21 days before the date of the on-site visit. Additional documents shall be submitted upon request of the peer-review team, within 7 days from the receipt of such requests.

7. Documents shall be provided in English unless otherwise agreed pursuant to paragraph 5. Where documents are not provided in English, the peer-review team may request that documents necessary to carry out the peer review be translated into English.

8. Before drawing up the peer-review report in accordance with Article 5, the peer-review team shall discuss preliminary findings with the peer-reviewed NCCA.

Article 5

Peer-review report

1. Within 21 days of the execution of the peer review, the peer-review team shall draw up a draft peer-review report, which shall include details of the Member State of the peer-reviewed NCCA, the peer-reviewer NCCAs, the Commission and any observer, as well as findings and conclusions of the peer review. Where necessary, the report shall include recommendations to enable improvement on the aspects covered by the peer review.
2. ENISA, in cooperation with the Commission and the ECCG, may develop a template for the peer-review report.
3. After drawing up the draft peer-review report in accordance with paragraph 1, the peer-review team shall provide it to the peer-reviewed NCCA for comments to be made within 14 days. The peer-review team shall evaluate the comments and, where possible, integrate them into the final report, with a view to ensuring consensus. In case of disagreement, the response of the peer-reviewed NCCA shall be annexed to the final report.
4. The final report shall be sent within two months from the execution of the peer-review to the ECCG, including a summary for publication. In accordance with Article 59(6) of Regulation (EU) 2019/881, the ECCG shall examine the report and endorse its summary, which shall be published on the website on European cybersecurity certification schemes created pursuant to Article 50 of Regulation (EU) 2019/881. The summary shall also include the response of the peer-reviewed NCCA or parts thereof, in agreement with the peer-reviewed NCCA.
5. The peer-review team shall anonymise personal data that it may have collected during the peer review before circulating the peer-review report outside of the peer-review team.

Article 6

Confidentiality

1. All parties involved in the peer reviews shall respect the confidentiality of information and data obtained in carrying out their tasks and activities in such a manner as to protect, in particular:
   (a) intellectual property rights and confidential business information or trade secrets of a natural or legal person, including source code, except the cases

referred to in Article 5 of Directive (EU) 2016/943 of the European Parliament and of the Council[3];

(b) the effective implementation of this Regulation;

(c) public and national security interests;

(d) integrity of criminal or administrative proceedings.

2. The peer-review team shall ensure that any information obtained through the peer-review process is handled securely. Once the final report and the summary referred to in Article 5(4) have been drawn up, the peer-review team, including any observer, shall delete or destroy all documents, other than the final report and the summary, that have been collected or generated as part of the peer-review process.

3. ENISA, taking into account existing best practices of the NCCAs, may, in cooperation with the ECCG, develop guidelines on secure and confidential communications.

Article 7

Capacity-building

ENISA shall analyse the aggregated results of the peer reviews and highlight lessons learned and best practices, in order to contribute to capacity-building for the NCCAs and to the maintenance of European cybersecurity certification schemes. That analysis may include, where appropriate, training and additional guidelines for NCCAs, developed in cooperation with the ECCG.

Article 8

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

[3] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L 157, 15.6.2016, p. 1) , ELI: http://data.europa.eu/eli/dir/2016/943/oj.

Done at Brussels,

For the Commission
The President
Ursula von der Leyen